4Н

УДК 004.415.24 (004.932)

О.Ю. Никитина
Институт кибернетики им. В.М. Глушкова НАН Украины, г. Киев
nikitinao@ukr.net

О методе цифровых водяных знаков на основе особенностей изображения и моментов Цернике

Рассматривается одна из задач компьютерной стеганографии – защита авторских прав на цифровые изображения. Описан метод на основе содержимого контейнера, стойкий к геометрическим искажениям. Проблема синхронизации ЦВЗ в изображении решается на основе особенностей изображения, выделенных с помощью детектора, использующего разницу в гауссианах. Моменты Цернике обеспечивают стойкость ЦВЗ к атакам удаления.

Введение

Задача защиты интеллектуальной собственности на сегодняшний день не только не теряет своей актуальности, но становится ещё более востребованной в виду непрерывного роста объёмов цифровой информации и более широкого использования Интернета. Распространение внедрения цифровых водяных знаков (ЦВЗ) в цифровые контейнеры для защиты прав собственности приводит к необходимости разработки методов, более стойких к активным атакам и естественным искажениям в канале обработки и передачи [1].

С развитием методов внедрения ЦВЗ атаки на стеганоконтейнеры становятся всё более замысловатыми. Активные атаки и естественные искажения могут привести к двум видам модификации контейнера-изображения: шумоподобные (изменение значений пикселов) и геометрические (пространственное изменение местоположения пикселов) [2].

К искажениям первого вида, в основном, приводят атаки, направленные на удаление водяного знака. Они основаны на предположении, что ЦВЗ является статистически описываемым шумом. К таким атакам относятся: шумовая фильтрация контейнеров, перемодуляция, сжатие с потерями (квантование), усреднение и коллизии. Большинство существующих систем ЦВЗ являются стойкими к этим атакам.

Геометрические атаки стремятся изменить ЦВЗ путем внесения пространственных или временных искажений. Геометрические атаки легко осуществимы и приводят к неэффективности многих систем ЦВЗ из-за потери синхронизации водяного знака в контейнере. Восстановление синхронизации требует применения специальных методов и является сложной задачей.

Если обеспечение стойкости к атакам удаления является более или менее решенной задачей, то обеспечение устойчивости к геометрическим атакам и локальным изменениям изображения все ещё мало изучено.

Метод, рассмотренный в статье, направлен на обеспечение стойкости к геометриическим атакам и относится к классу методов, использующих содержимое контейнера.

Подходы к противодействию геометрическим атакам на ЦВЗ

Цифровое изображение $I(x, y)$ представляет собой массив чисел, соответствующих уровням яркости точек (пикселов) изображения на углах двумерной сетки (рис. 1).

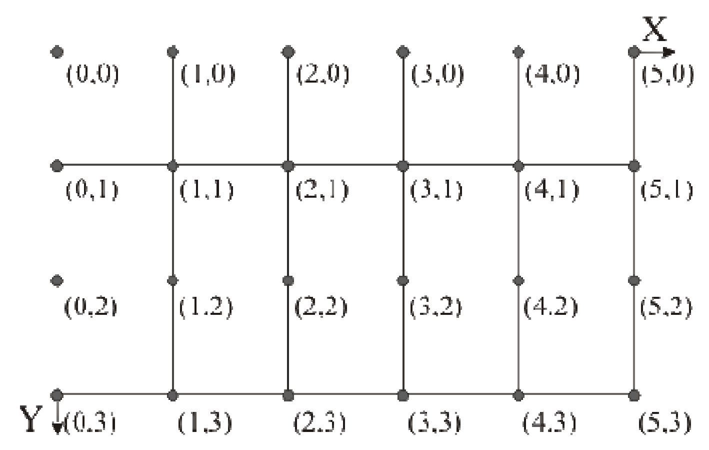


Рисунок 1 – Представление цифрового изображения

Геометрические атаки описываются различными математическими моделями [3]. Удобным является использование однородных координат, которые позволяют унифицировать запись координат точек в пространстве. Однородными координатами точки $P(x, y)$, $P \in R^2$ называются координаты $P_{\text{hom}} = (wx, wy, w)$, $P \in R^3$ причём хотя бы один элемент должен быть отличен от нуля. Аффинное преобразование при однородных координатах может быть выражено с помощью одного матричного умножения как

$$\begin{bmatrix} x' \\ y' \\ 1 \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & t_x \\ a_{21} & a_{22} & t_y \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ 1 \end{bmatrix}.$$

Аффинное преобразование имеет шесть степеней свободы: две для перемещения (t_x, t_y) и по одной для вращения, масштабирования, изменения пропорций (растяжения) и деформации сдвигом $(a_{11}, a_{12}, a_{21}, a_{22})$.

Общее перспективное преобразование с помощью однородных координат записывается как

$$\begin{bmatrix} w'x' \\ w'y' \\ w' \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & 1 \end{bmatrix} \begin{bmatrix} wx \\ wy \\ w \end{bmatrix}.$$

Два дополнительных коэффициента a_{31} и a_{32} описывают перспективную проекцию. К геометрическими атакам также относятся усечение (обрезка), перестановка местами отдельных пикселов или строк, бочкообразные искажения и др.

В результате геометрических атак исходное изображение преобразовывается. Координаты пикселов исходного изображения изменяются и не соответствуют узлам наложенной двумерной сетки (рис. 2). Значения уровней яркостей пикселов интерполируется, что ещё более усложняет задачу построения системы ЦВЗ, стойкой к геометрическим атакам.

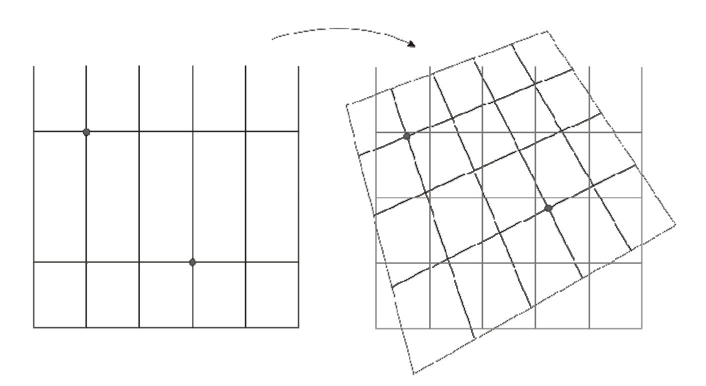


Рисунок 2 – Иллюстрация пространственного преобразования пикселов изображения

Наиболее простой подход обеспечения стойкости к геометрическим атакам заключается в использовании закрытой системы ЦВЗ [1]. В этом случае для восстановления синхронизации требуется исходный контейнер и ЦВЗ. Такая система обеспечивает наибольшую устойчивость к активным атакам, однако требует значительных вычислительных затрат. Требование наличия исходного изображения при детектировании сильно ограничивает область применения методов на основе такой схемы. Промежуточным вариантом является использование полузакрытой системы: при детектировании используется только исходный ЦВЗ. Наиболее предпочтительной, но сложной в реализации, является открытая система, которая не требует наличия исходных данных.

Рассмотрим наиболее характерные подходы западных исследователей к обеспечению стойкости к геометрическим атакам.

Один из подходов основывается на выделении областей, инвариантных к определённому виду геометрических преобразований. Зачастую такие методы основаны на свойствах преобразования Фурье – Меллина [4]. Основным недостатком при использовании подхода внедрения ЦВЗ на основе преобразования Фурье – Меллина является снижение качества изображения вследствие интерполяции значений уровней яркостей пикселей. В работе [5] предложен подход построения системы ЦВЗ, стойкой к смещению, масштабированию и вращению. В этом подходе решена проблема сохранения приемлемого качества маркированного изображения.

Использование дополнительной информации при внедрении ЦВЗ расширяет возмоности решения задачи стойкости к геометрическим атакам. Одним из видов дополнительной информации может быть шаблон – совокупность пиков, вложенных в пространственную или частотную область изображения. Наиболее часто шаблон получается увеличением значений коэффициентов средних частот амплитудного спектра Фурье контейнера, выбранных в пределах определённой области, т.е. созданием локальных пиков. Шаблон позволяет произвести оценку геометрических преобразований. Выигрывая в простоте, методы на базе шаблона могут себя дискредитировать. Шаблон легко обнаруживается с помощью фильтрации и может стать отправным пунктом для активной атаки. Кроме того, шаблон привносит дополнительный шум в изображение [6].

Структурный (или самоопорный) ЦВЗ является модулирующей функцией и внедряется в пространственную область изображения линейно, периодически и с различными смещениями [7]. Такое внедрение ЦВЗ изменяет автокорреляцию маркированного изображения, добавляя многократные пики. Геометрические преобразования меняют периодичность пиков в функции автокорреляции. Изменение позиций пиков восстановленного цифрового изображения даёт возможность определить параметры геометрических искажений и выполнить их компенсацию. Структурные ЦВЗ являются стойкими к обобщенным геометрическим преобразованиям, не вносят дополнительных шумов в изображение, но разрушаются при удалении пиков корреляции. Они имеют ограниченную стойкость к локальным искажениям.

Системы ЦВЗ, использующие содержимое контейнера

Подход к обеспечению стойкости ЦВЗ к геометрическим атакам, в котором используется содержимое (контекст) контейнера, более перспективный и относится ко второму поколению систем ЦВЗ [8]. Основная идея состоит в определении особых областей и точек контейнера, с последующим внедрением в их окрестностях невидимого и стойкого ЦВЗ.

Особой точкой f_p называется точка, окрестность которой отличается от окрестностей близлежащих точек по выбранной мере

$$\left\{ \forall f : \left| f_p - f \right| < r \to \tau(\Omega_f, \Omega_{f_p}) > \varepsilon \right\},$$

где Ω_f – окно поиска в центре с точкой f, $\tau(\Omega_f, \Omega_{f_p})$ – функция гладкости градиента цветовой компоненты в окне поиска.

Использование оригинальных данных стегоконтейнера позволяет решить задачу восстановления синхронизации ЦВЗ. Решение о применённых геометрических атаках может быть принято на основе информации об особых точках. Местоположение водяного знака связывается не с пространственными координатами пикселов изображения, а с контекстом изображения. Надёжность методов зависит непосредственно от точности определения детектором тех же самых особых точек (областей) после проведённых геометрических атак.

Нахождение особых точек (областей) является важной начальной стадией обработки изображения. Обычно на этой стадии вычисляются локальные экстремальные точки (области) изображения на основе цветовых компонентов градиента яркости. Существуют различные типы особых точек (областей): точки, контуры объектов, текстурированные области. Для нахождения особенностей используют функции-детекторы разных видов [9-11]. Для достижения устойчивости ЦВЗ к геометрическим искажениям, на этапе выделения особых точек (областей), необходимо использовать детектор, инвариантный к определённому виду преобразований.

В данной работе предлагается использование в качестве детектора функции разницы в гауссианах, как функций от координат пикселов (Different of Gaussian). Цифровой водяной знак формируется с использованием нормализованного момента Цернике $\{Z_{nm}\}$ [12]:

$$Z_{nm} = \frac{n+1}{\pi} \sum_n \sum_m I(x,y) V_{nm}^*(x,y), \qquad (1)$$

где $I(x,y)$ – цифровое изображение; n – неотрицательное целое число, порядок момента; m – целое число, причём $n - |m| \geq 0$ и чётное; $V_{nm}(x,y)$ – комплексная функция определённая как

$$V_{nm}(x,y) = V_{nm}(\rho,\theta) = R_{nm}(\rho)\exp(jm\theta).$$

$\rho = \sqrt{x^2 + y^2}$, $\theta = tg^{-1}(y/x)$; $R_{nm}(\rho)$ – радиальный полином вида:

$$R_{nm}(\rho) = \sum_{s=0}^{(n-|m|)/2} (-1)^s \cdot \frac{(n-s)!}{s!(\frac{n+|m|}{2} - s)!(\frac{n-|m|}{2} - s)!} \rho^{n-2s}.$$

Алгоритм внедрения ЦВЗ

Представим пошаговое описание рассматриваемого метода.

Алгоритм внедрения ЦВЗ.

1. Нахождение особых точек.
2. Определение характеристик окрестностей выбранных особых точек.
3. Вычисление нормализованного момента Цернике в каждой окрестности.
4. Генерация водяного знака путём модификации вычисленных нормализованных моментов Цернике.
5. Маркировка изображения.

Алгоритм обнаружения ЦВЗ.

1. Нахождение особых точек (аналогично внедрению).
2. Вычисление окрестностей особых точек с использованием дескрипторов, определённых в контейнере.
3. Синхронизация окрестностей особых точек.
4. Вычисление нормализованного момента Цернике для каждой окрестности особой точки.
5. Обнаружение ЦВЗ по пикам в разнице моментов Цернике.

Рассмотрим более детально процесс выделения особых точек.

Для нахождения особых точек используются масштабные представления изображений. Вопросу масштабирования пространства и масштабным преобразованиям уделялось большое внимание во второй половине XX века. Большим вкладом была работа [13], идеи которой в дальнейшем получили существенное развитие [14]. Масштабное преобразование изображения является представлением изображения на разных уровнях сглаживания (рис.3).

Сглаживающим фильтром является гауссова функция, ординатами которой служат координаты пиксела

$$G(x,y,\sigma)=\frac{1}{2\pi\sigma^2}e^{-(x^2+y^2)/2\sigma^2}, \qquad (2)$$

σ – среднеквадратическое отклонение гауссианы, измеряемое в расстояниях между пикселами.

Для получения ряда сглаженных изображений $L(x,y,\sigma)$, в каждой точке изображения $I(x,y)$ вычисляется свёртка с гауссовым яром:

$$L(x,y,\sigma)=G(x,y,\sigma)\cdot I(x,y) \qquad (3)$$

для разных значений σ. Далее вычисляется разница в гауссианах

$$D(x,y,\sigma)=\left|L(x,y,\sigma_1)-L(x,y,\sigma_2)\right|. \qquad (4)$$

Схема построения масштабного представления изображения представлена на рис. 4. Выполняется последовательная свёртка изображения с шагом $\sigma,\sigma^2,\sigma^4,...,\sigma^n$ ($n=r^2$, $r\in Z$) согласно выражению (3). Для полученного набора изображений (слева на рисунке) вычисляется разница в гауссианах смежных изображений согласно выражению (4) (справа на рисунке).

Иллюстрация отфильтрованного сглаживающим фильтром тестового изображения Cameraman и разница в гауссианах исходного изображения с полученным представлена на рис. 5.

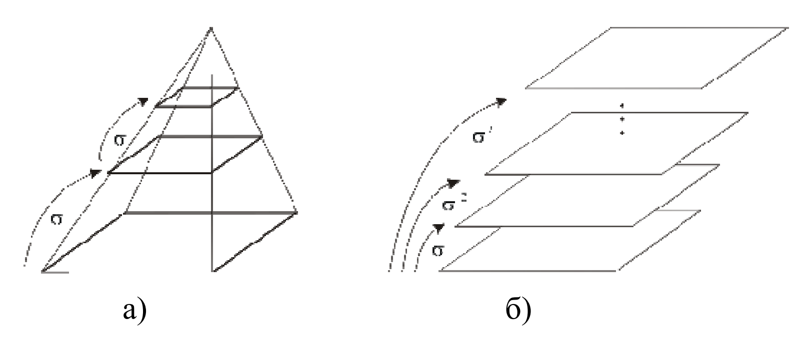


Рисунок 3 – Масштабные представления: а) пирамидальное представление, образованное сглаживанием и дискретизацией, б) масштабное представление, образованное последовательным сглаживанием изображения

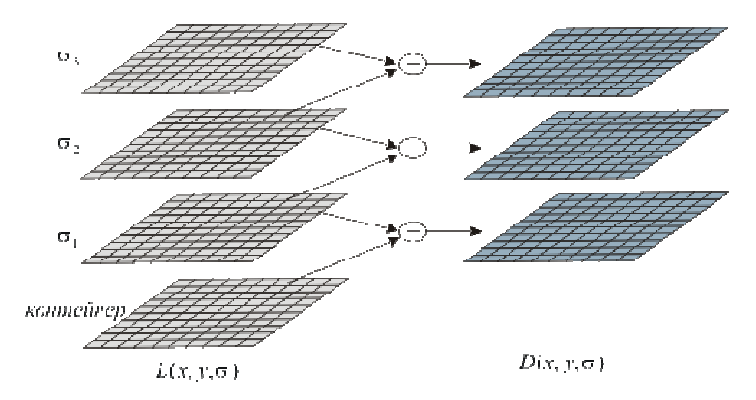


Рисунок 4 – Схема построения масштабного представления изображения

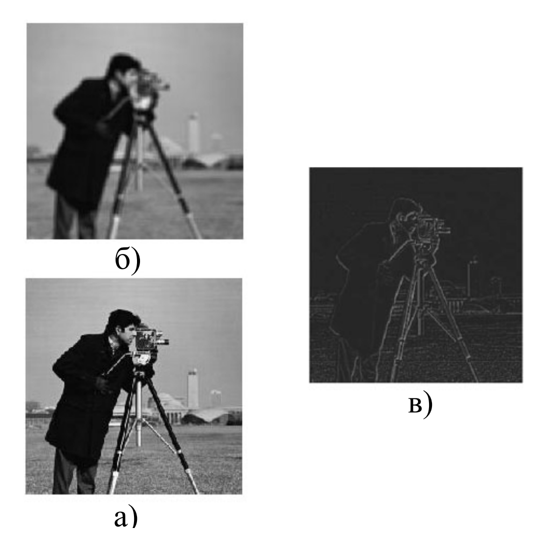


Рисунок 5 – Тестовые изображения Cameraman:
а) исходное изображение; б) изображение $L(x,y,\sigma)$; в) изображение $D(x,y,\sigma)$

Находятся экстремальные точки изображения, которые являются претендентами на особы точки. Для этого вокруг каждой k-ой точки изображения $D(x,y,\sigma_i)$ рассматривается окрестность заданного радиуса. Если в этой окрестности существует точка k_1, уровень освещённости которой больше, чем у k-ой точки, k-ую точку исключаем из дальнейшего рассмотрения, и переходим к рассмотрению k_1-ой точки. Если в заданной окрестности k-ой точки не существует точки, уровень освещённости которой превышает уровень освещённости k-ой точки, тогда она назначается локальным максимумом.

Схематично процесс нахождения экстремумов показан на рис. 6.

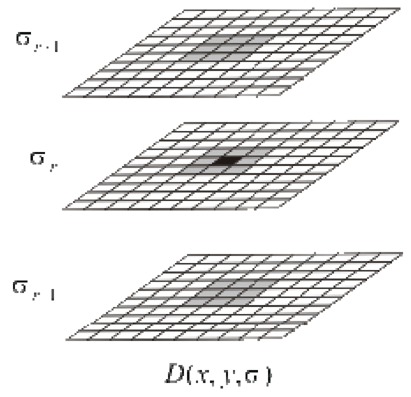


Рисунок 6 – Схема нахождения экстремальных точек в смежных изображениях

Найденные точки являются неустойчивыми и неточными, поэтому необходимо выполнить их уточнение. Уточнение проводится устранением точек с малым контрастом или расположенных вдоль контура.

Для каждого уровня дискретизации вычисляется матрица вида:

$$H = \begin{bmatrix} D_{xx} & D_{xy} \\ D_{xy} & D_{yy} \end{bmatrix}, \qquad (5)$$

где D_{xx}, D_{xy}, D_{yy} – вторые частные производные функции $D(x, y, \sigma)$. Тогда стабильность положения точек может быть определена из неравенства:

$$S = \frac{(D_{xx} + D_{yy})^2}{D_{xx}D_{xy} - D_{xy}^2} < \frac{(r+1)^2}{r},$$

где r – соотношение между наибольшим и наименьшим собственными значениями матрицы (5).

Следующим шагом является определение характеристик локальных фрагментов изображения вблизи особых точек (областей) – дескрипторов. Особые точки (области), полученные разными детекторами, отличаются локализацией, размером, структурой и информационным содержанием (в конечном счёте – дескрипторами).

Влияние аффинных преобразований на основные параметры окрестности особой точки (местоположение, масштаб, форма) имеет решающее значение для принятия решения о применённой геометрической атаке. Местоположение определяется координатами особой точки относительно начала координат. Радиус ε-окрестности особой точки (p_1, p_2) связан с уровнем разрешения изображения и влияет на точность детектора при повторном определении особой точки в стеганоконтейнере. Рекомендуемый диапазон значений ε (2;10). Окрестность особой точки определяется по формуле:

$$(x^2 - p_1)^2 + (y - p_2)^2 = (k\varepsilon)^2, \qquad (6)$$

где k – коэффициент, связанный с радиусом окрестности.

Окрестности особых точек не должны пересекаться между собой.

На следующем шаге для установления дескриптора в каждой точке окрестности вычисляется значение градиента $m(x, y)$ и направление вектора градиента $\varphi(x, y)$:

$$m(x, y) = \sqrt{(L(x+1, y) - L(x-1, y))^2 + (L(x, y+1) - L(x, y-1))^2}$$

$$\varphi(x, y) = \tan^{-1}\frac{L(x, y+1) - L(x, y-1)}{L(x+1, y) - L(x-1, y)}.$$

Более детально процедура описана в работе [11].

В полученном наборе дескрипторов исходного изображения содержится ключевая информация относительно окрестностей особых точек. Полученные окрестности инвариантны к повороту и масштабированию.

Для каждой окрестности особой точки вычисляются значения $\{Z_{nm}\}$. Из полученных значений формируется водяной знак:

$$I(x, y) = \sum_{n=0}^{N_{\max}} \sum_{m=-n}^{n} \tilde{Z}_{nm} V_{nm}(x, y), \qquad (7)$$

где $N_{\max}$ – максимальная степень моментов Цернике, $\tilde{Z}_{nm}$ – модифицированные значения моментов.

Схема внедрения ЦВЗ показана на рис. 7.

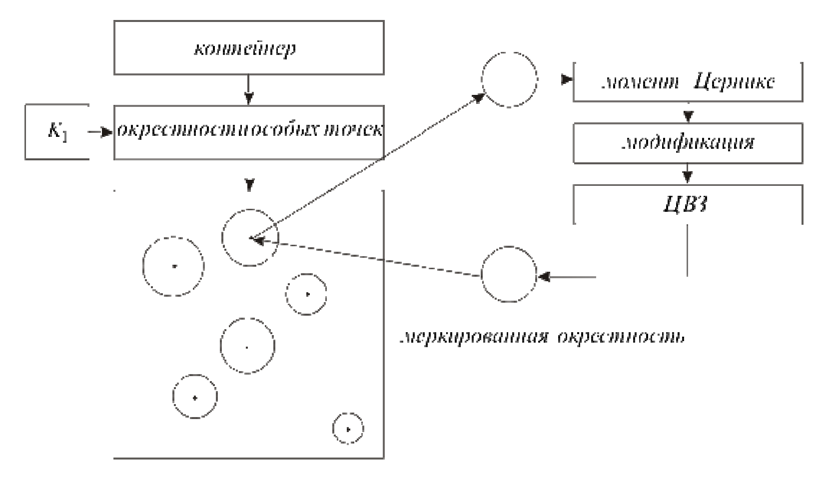


Рисунок 7 – Схема внедрения ЦВЗ

Обнаружение ЦВЗ

Для обнаружения цифрового водяного знака в изображении, подвергнувшегося геометрической атаке, находят особые точки и определяют их окрестности, используя дескрипторы контейнера. Синхронизация осуществляется по формуле (6). Разница моментов Цернике, вычисленных для исходного и исследуемого изображений, используется для определения пиков, которые указывают на присутствие водяного знака (рис. 8).

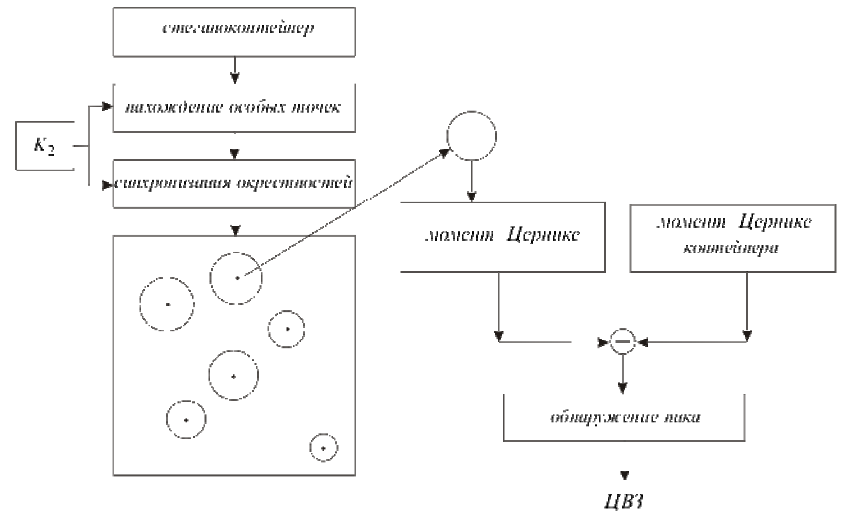


Рисунок 8 – Схема обнаружения ЦВЗ

Выводы

Несмотря на то, что рассмотренная схема не является открытой, для обнаружения водяного знака требуются только значения дескрипторов пустого контейнера и моменты Цернике, рассчитанные для окрестностей особых точек. Описанный алгоритм позволяет синхронизировать большинство окрестностей особых точек и выявить водяной знак. Схема является стойкой к вращению, масштабированию, локальному усечению (до 50 %). Стойкость к локальному усечению обеспечивается множественным внедрением водяного знака. При уменьшении изображения схема менее стойкая к масштабированию из-за информационных потерь.

Литература

1. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. –М.: СОЛОН-Пресс, 2002. – 261 с.
2. Кошкина Н.В., Никитина О.Ю. К вопросу о защите интеллектуальной собственности на бумажных носителях // Искусственный интеллект. – 2006. – № 3. – С. 757-763.
3. Яне Б. Цифровая обработка изображений. – М.: Техносфера, – 2007. – 583 с.
4. Zheng D., Zhao J., Saddik A. RST Invariant Digital Image Watermarking Based on Log-Polar Mapping and Phase Correlation // IEEE Transactions on Circuits and Systems for Video Technology, 2003. – 13, Is. 8. – P. 753-765.
5. Никитина О.Ю. Оптимизация по точности методов цифровых водяных знаков, основанных на преобразовании Фурье – Меллина // Искусственный интеллект. – 2007. – № 4. – С. 335-341.
6. Voloshynovskiy S., Herrigel A., Rytsar Y.B. Watermark template attack // Proc. of the SPIE: Security and Watermarking of Multimedia Content III. – California (USA) 2001. – Vol. 4314. – P. 394-400.
7. Kutter M. Watermarking resisting to translation, rotation and scaling // Proc. of the SPIE: Multimedia Systems and Appl. – Boston (USA) 1998. – Vol. 3528. – P. 423-431.
8. Kutter M., Bhattacharjee S.K., Ebrahimi T. Toward second generation watermarking schemes // Proc. of International Conference on Image Processing. – 1999. – Vol. 1. – P. 320-323.
9. Canny J. A computational approach to edge detection // IEEE Trans. Pattern Analysis and Machine Intelligence. – 8. – 1986. – P. 679-714.
10. Harris C., Stephens M. A combined corner and edge detector // Proceedings of the 4th Alvey Vision Conference. – 1988. – P. 147-151.
11. Lowe D.G. Distinctive image features from scale-invariant keypoints // International Journal of Computer Vision. – 2004. – No. 2. – P. 91-110.
12. Hse H., Newton A.R. Sketched symbol recognition using Zernike moments // Pattern Recognition. ICPR 2004. Proceedings of the 17th International Conference. – 2004. – Vol. 1. – P. 367- 370.
13. Witkin A. Scale-space filtering // International joint conference on artificial intelligence. – 1983. – P. 1019-1022.
14. Koenderink J., Doorn A. Dynamic shape // Biological cybernetics. – 1986. – № 58. – P. 383-396.

О.Ю. Нікітіна

Про метод цифрових водяних знаків на основі особливостей зображення та моментів Церніке

Розглядається одна із задач комп’ютерної стеганографії – захист авторських прав на цифрові зображення. Описаний метод на основі контенту контейнера, що є стійким до геометричних спотворень. Проблема синхронізації ЦВЗ в зображенні розв’язується на основі особливостей зображення. Особливості виділені за допомогою детектора, що використовує різницю в гаусіанах. Моменти Церніке забезпечують стійкість ЦВЗ до атак видаленням.

O.Yu. Nikitina

About the Digital Watermark Method Feature-Based Image and Zernike Moments

One problem of computer steganography is considered in the paper – digital image copyright interests. The container content-based method is described that is geometric effect robust. The synchronization in the image problem solution is image feature-based that were detected by the using difference of Gaussians detector. Zernike moments are protecting watermark from deletion attacks.

Статья поступила в редакцию 21.07.2008.